

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) A method for secure key delivery for decrypting a
2 distribution archive file containing a plurality of digital content documents at an
3 unsecured site that receives a stream of distribution archive files from a
4 publishing site, the method comprising:
 - 5 (a) at the publishing site, encrypting each digital content document with a key
6 to generate encrypted document content;
 - 7 (b) at the publishing site, computing for each document a document identifier
8 that is ~~related to~~ computed from, but cannot be derived solely from, the
9 encrypted content of that document;
 - 10 (c) at the publishing site, creating a list of document identifier and decryption
11 key pairs;
 - 12 (d) at the publishing site, assembling the encrypted document content for
13 each content document and the key pair list into a distribution archive file;
 - 14 (e) at the publishing site, encrypting the distribution archive file with a
15 scheduled key unique to that distribution archive file and placing the
16 encrypted distribution file on the stream;
 - 17 (f) at the unsecured site, selecting a distribution archive file from the stream;
 - 18 (g) at the unsecured site, extracting a scheduled key from the selected
19 distribution archive file in the stream;
 - 20 (h) at the unsecured site, using the extracted scheduled key to decrypt the
21 next subsequent distribution archive file in the stream following the
22 selected distribution archive file;

23 (i) removing the encrypted document content and the key pair list from the
24 decrypted distribution archive file and storing them at the unsecured site;
25 and
26 (j) selecting the distribution archive file decrypted in step (h) and repeating
27 steps (g), (h), (i) and (j) for each distribution archive file in the stream.

1 2. (Previously Presented) The method of claim 1 further comprising:

2 (k) receiving a scheduled key at the unsecured site to decrypt the first
3 distribution archive file in the stream from the publishing site.

1 3. (Previously Presented) The method of claim 1 wherein step (e) comprises
2 encrypting, with a scheduled key, a distribution archive file including a scheduled
3 key for the next distribution archive file in the stream and the plurality of
4 encrypted content files.

1 4. (Previously Presented) The method of claim 1 wherein step (e) comprises
2 encrypting, with a scheduled key, a distribution archive file including the plurality
3 of encrypted content files and a non-encrypted scheduled key for the next
4 distribution archive file.

5. (Canceled).

1 6. (Previously Presented) The method of claim 1 wherein step (e) comprises
2 generating a new scheduled key, encrypting the new scheduled key and
3 including the encrypted scheduled key in the distribution archive file.

1 7. (Previously Presented) The method of claim 1 wherein step (b) comprises for
2 each document, computing the document identifier using a text string embedded
3 in program code in the publishing site.

- 1 8. (Previously Presented) The method of claim 1 wherein step (g) comprises storing
2 an extracted scheduled key in encrypted form.
- 1 9. (Previously Presented) The method of claim 7 further comprising recomputing a
2 document identifier at the unsecured site with a text string embedded in program
3 code located at the unsecured site.
- 1 10. (Previously Presented) The method of claim 9 wherein the text string embedded
2 in program code in the publishing site is the same as the text string embedded in
3 program code at the unsecured site.
- 1 11. (Currently Amended) An apparatus for secure key delivery for decrypting a
2 distribution archive file containing a plurality of digital content documents at an
3 unsecured site that receives a stream of distribution archive files from a
4 publishing site, the apparatus comprising:
5 at the publishing site, an encryption engine that encrypts each digital
6 content document with a key to generate encrypted document content;
7 at the publishing site, an OID calculator that computes for each document
8 a document identifier that is ~~related to~~ computed from, but cannot be derived
9 solely from, the encrypted content of that document;
10 at the publishing site, means for creating a list of document identifier and
11 decryption key pairs;
12 at the publishing site, means for assembling the encrypted document
13 content for each content document and the key pair list into a distribution archive;
14 at the publishing site, means for encrypting the distribution archive file with
15 a scheduled key unique to that distribution archive file;
16 at the unsecured site, a key decryptor that extracts a scheduled key from
17 each distribution archive file in the stream;
18 means for temporarily storing the extracted scheduled key at the
19 unsecured site;

20 at the unsecured site, a decryption engine that uses the stored scheduled
21 key to decrypt the next distribution archive file in the stream following the
22 distribution archive file from which the scheduled key was extracted; and
23 a file system that removes the encrypted document content and the key
24 pair list from the decrypted archive file and stores them at the unsecured site.

1 12. (Original) The apparatus of claim 11 further comprising means for receiving a
2 scheduled key for the first distribution archive file in the stream from the
3 publishing site.

1 13. (Previously Presented) The apparatus of claim 11 wherein the apparatus further
2 comprises an encryption engine that encrypts, with a scheduled key, a
3 distribution archive file including a scheduled key for the next distribution archive
4 file in the stream and the plurality of encrypted content files.

1 14. (Previously Presented) The apparatus of claim 11 wherein the apparatus further
2 comprises an encryption engine that encrypts, with a scheduled key, a
3 distribution archive file including the plurality of encrypted content files and a non-
4 encrypted scheduled key for the next distribution archive file.

15. (Canceled).

1 16. (Previously Presented) The apparatus of claim 11 wherein the means for
2 encrypting the distribution archive with a scheduled key comprises a key
3 generator that generates a new scheduled key, a key encryptor that encrypts the
4 new scheduled key and means for including the encrypted scheduled key in the
5 distribution archive.

- 1 17. (Previously Presented) The apparatus of claim 11 wherein the OID calculator
2 encrypts the new scheduled key using a text string embedded in program code in
3 the publishing site.
- 1 18. (Previously Presented) The apparatus of claim 11 wherein the means for
2 temporarily storing the extracted scheduled key comprises means for storing an
3 extracted scheduled key in encrypted form.
- 1 19. (Previously Presented) The apparatus of claim 17 further comprising means for
2 recomputing a document identifier with a text string embedded in program code
3 located at the unsecured site.
- 1 20. (Previously Presented) The apparatus of claim 19 wherein the text string
2 embedded in program code in the publishing site is the same as the text string
3 embedded in program code at the unsecured site.
- 1 21. (Currently Amended) A computer program product for secure key delivery for
2 decrypting a distribution archive file containing a plurality of digital content files at
3 an unsecured site that receives a stream of distribution archive files from a
4 publishing site, the computer program product comprising a computer usable
5 medium having computer readable program code thereon, including:
6 program code at the publishing site, for encrypting each digital content
7 document with a key to generate encrypted document content;
8 program code at the publishing site, for computing for each document a
9 document identifier that is ~~related to~~ computed from, but cannot be derived solely
10 from, the encrypted content of that document;
11 program code at the publishing site, for creating a list of document
12 identifier and decryption key pairs;

13 program code at the publishing site, for assembling the encrypted
 14 document content for each content document and the key pair list into a
 15 distribution archive file; and
 16 program code at the publishing site, for encrypting the distribution archive
 17 file with a scheduled key unique to that distribution archive file and for placing the
 18 encrypted distribution file on the stream;
 19 program code at the unsecured site for extracting a scheduled key from
 20 each distribution archive file in the stream;
 21 program code at the unsecured site for temporarily storing the extracted
 22 scheduled key;
 23 program code at the unsecured site for using the stored scheduled key to
 24 decrypt the next distribution archive file in the stream following the distribution
 25 archive file from which the scheduled key was extracted; and
 26 program code for removing the encrypted document content and the key
 27 pair list from the decrypted archive file and for storing them at the unsecured site.

1 22. (Original) The computer program product of claim 21 further comprising program
 2 code for receiving a scheduled key for the first distribution archive file in the
 3 stream from the publishing site.

1 23. (Previously Presented) The computer program product of claim 21 wherein the
 2 computer program product further comprises:
 3 program code for encrypting, with a scheduled key, a distribution archive
 4 file including a scheduled key for the next distribution archive file in the stream
 5 and the plurality of encrypted content files.

1 24. (Previously Presented) The computer program product of claim 21 wherein the
 2 computer program product further comprises:

3 program code for encrypting, with a scheduled key, a distribution archive
4 file including the plurality of encrypted content files and a non-encrypted
5 scheduled key for the next distribution archive file.

25. (Canceled).

1 26. (Previously Presented) The computer program product of claim 21 wherein the
2 program code for encrypting the distribution archive file comprises program code
3 for generating a new scheduled key, program code for encrypting the new
4 scheduled key and program code for including the encrypted scheduled key in
5 the distribution archive file.

1 27. (Previously Presented) The computer program product of claim 21 wherein the
2 program code for computing a document identifier computes the document
3 identifier using a text string embedded in program code in the publishing site.

1 28. (Previously Presented) The computer program product of claim 21 wherein the
2 program code for temporarily storing the extracted scheduled key comprises
3 program code for storing an extracted scheduled key in encrypted form.

1 29. (Previously Presented) The computer program product of claim 28 further
2 comprising program code for recomputing a document identifier with a text string
3 embedded in program code located at the unsecured site.

30. (Previously Presented) The computer program product of claim 29 wherein the
 text string embedded in program code in the publishing site is the same as the
 text string embedded in program code at the unsecured site.